# Quantum communication without alignment using multiple-qubit single-photon states

L. Aolita and S. P. Walborn
*Instituto de Física, Universidade Federal do Rio de Janeiro, Caixa Postal 68528, Rio de Janeiro, RJ 21941-972, Brazil*
(Dated: February 1, 2008)

We propose a scheme for encoding logical qubits in a subspace protected against collective rotations around the propagation axis using the polarization and transverse spatial degrees of freedom of single photons. This encoding allows for quantum key distribution without the need of a shared reference frame. We present methods to generate entangled states of two logical qubits using present day down-conversion sources and linear optics, and show that the application of these entangled logical states to quantum information schemes allows for alignment-free tests of Bell's inequalities, quantum dense coding and quantum teleportation.

PACS numbers: 03.67.-a, 03.67.Dd, 03.67.Hk



The most common implementations of quantum communication schemes involve two or more parties that, in order to encode and decode information, must share a common spatial reference frame. Nevertheless, it has been pointed out that a shared reference frame (SRF) is a resource that should not be taken for granted, since establishing a perfect SRF requires the transmission of an infinite amount of information [1]. One can circumvent the need for a SRF encoding logical qubits in multi-qubit states with appropriate symmetry properties, so that the states are rotationally invariant. This results in a considerable reduction in overhead due to initial alignment stages; but, since all the available protocols exploiting multi–qubit states of photons require the use of two [2, 3, 4], three [5], or four photons [5, 6, 7, 8] to encode one single logical qubit, this increases the amount of resources as well as the sensitivity of the protocol to photon losses.

The lack of alignment between two users of a protocol is equivalent to a collective random rotation of the qubits during the transmission process, which can be considered as a special type of collective noise. Rotationally invariant states, in turn, span a decoherence-free subspace (DFS) protected against such noise. A DFS protected against collective noise is a subspace of the total Hilbert space of a system that is immune to decoherence, provided that it acts identically and simultaneously on each member of the system [9]. For example, two ions of the same species closely spaced in a Paul trap, or photons propagating close together in the same optical fiber, are exposed approximately to the same fluctuations. Thus, through the use of DFSs, their respective coherence properties can be enhanced considerably [4, 10]. Nevertheless, the assumption of collective noise is in practice fulfilled only approximately, as two different particles are never actually subject to exactly the same noise.

Photons are a natural candidate for quantum communication due to the ease with which they can be transmitted. Using spontaneous parametric down-conversion (SPDC), one can create triggered single photons or entangled photon pairs [11, 12]. Also, there has been a great deal of recent work exploiting the fact that one can encode multiple qubits into multiple degrees of freedom (DOF) of photons [12, 13]. But as different DOF are not necessarily affected in the same way by the same rotation, the collective rotation hypothesis is not necessarily valid, even for different DOF of the same single photon.

However, there do exist two DOF of the photon that play a preferential role for alignment-free quantum communication: the lack of a common reference frame in the plane orthogonal to the propagation direction does imply a collective rotation for the polarization and the transverse spatial DOF. Here we show that it is possible to encode logical qubits into single photons using these two DOF, which allows for the implementation of quantum information protocols in free space without the need of aligning the two directions orthogonal to the propagation axis. The novel aspect here is that the rotationally invariant states are carried by single photons, which not only reduces the required resources, but also the damage due to photon losses. We first present the encoding scheme and then discuss the implementation of several quantum communication protocols.

Let us outline the scenario. Two users, $A$ and $B$, wish to communicate photonic qubits. We assume that, in order to send and detect the photons, they have previously established a common propagation direction by, for example, using an intense laser beam. Our scheme is based on the fact that, in the usual paraxial approximation, both the polarization and transverse spatial modes of a field are defined in the plane transverse to the propagation direction of the field. For example, consider a photon prepared in the state $|\psi_A\rangle = \alpha |H_A\rangle + \beta |V_A\rangle$, where $|H_A\rangle$ and $|V_A\rangle$ refer to the horizontal and vertical polarization directions in reference frame $A$. A second user $B$ whose coordinate system is rotated an angle $\theta$ around the propagation axis, would describe this state as $|\psi_B\rangle = \alpha(\cos\theta |H_B\rangle + \sin\theta |V_B\rangle) + \beta(\cos\theta |V_B\rangle - \sin\theta |H_B\rangle)$.

Similarly, one can encode information in the transverse spatial DOF of a photon using the Hermite Gaussian

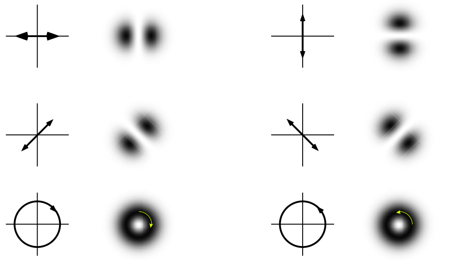

FIG. 1: Polarization and HG modes of the electromagnetic field. Top: horizontal polarization $|H\rangle$ and $\mathrm{HG}_{01}$ mode $|h\rangle$ (left), vertical polarization $|V\rangle$ and $\mathrm{HG}_{10}$ mode $|v\rangle$ (right). Center: diagonal polarizations $(|H\rangle \pm |V\rangle)/\sqrt{2}$ and diagonal modes $(|h\rangle \pm |v\rangle)/\sqrt{2}$. Bottom: circular polarizations $(|H\rangle \pm i\,|V\rangle)/\sqrt{2}$ and circular modes $(|h\rangle \pm i\,|v\rangle)/\sqrt{2}$.

(HG) modes, denoted $\mathrm{HG}_{nm}$, where the positive integers $n$ and $m$ are the horizontal and vertical indices with respect to some coordinate system. Here we consider the first order modes ($n+m=1$) $\mathrm{HG}_{01}$ and $\mathrm{HG}_{10}$, which form a basis analogous to that of polarization [14], and are described relative to its same reference frame, as FIG. 1 shows. That is if a user $A$ can prepare an arbitrary quantum state $|\Psi_A\rangle = \alpha\,|h_A\rangle + \beta\,|v_A\rangle$, where $h_A$ ($v_B$) represents a horizontally (vertically) aligned mode $\mathrm{HG}_{10}$ ($\mathrm{HG}_{01}$), then a $\theta$-rotated user $B$ would describe this state as $|\Psi_B\rangle = \alpha(\cos\theta\,|h_B\rangle + \sin\theta\,|v_B\rangle) + \beta(\cos\theta\,|v_B\rangle - \sin\theta\,|h_B\rangle)$. Since the effect of a rotated user is the same for both DOF, the assumption of collective rotation, around the propagation axis, is fulfilled exactly; and it is thus possible to construct rotationally invariant single photon states which form a basis for a logical qubit.

We define our single-photon logical computational basis $B_L$ using the same abstract encoding of [2, 10]: $B_L = \{|0_L\rangle \equiv (|Hv\rangle - |Vh\rangle)/\sqrt{2},\ |1_L\rangle \equiv (|Hh\rangle + |Vv\rangle)/\sqrt{2}\}$, where the subindex $L$ stands for "logical". Here lowercase (uppercase) letters refer to HG (polarization) modes; *e.g.* $|Hv\rangle$ stands for a photon with polarization $H$ and transverse mode $v$, etc. All states in the subspace $\mathbb{V}_{DFS}$, generated by $B_L$, are invariant under arbitrary rotations of the reference frame around the propagation axis. These states are single-photon Bell states, and are easily prepared and detected unambiguously with perfect efficiency using single photon controlled-not ($c\hat{\sigma}^x$) gates, which have been constructed using relatively simple linear optical devices [8], and subsequently measuring in the physical basis using polarizing beam splitters (PBS) and transverse mode sorters (MS)[15].

Also one can manipulate the physical qubits individually using a combination of half- and quarter-wave plates, in the case of polarization, or Dove prisms and mode converters, in the case of HG modes [14, 16]. Using these elements and the interferometric techniques described in Refs. [8], one can implement any controlled-logic operation among the physical qubits, and consequently, implement any $SU(2)$ unitary operation on the logical qubit. For example, using a half-wave plate (HWP) aligned at $\phi/2$, followed by a HWP aligned at $0°$, realizes the polarization rotation $\hat{R}^y_p(2\phi)$: $|H\rangle \longrightarrow \cos\phi\,|H\rangle + \sin\phi\,|V\rangle$, $|V\rangle \longrightarrow -\sin\phi\,|H\rangle + \cos\phi\,|V\rangle$. Under this physical transformation the logical states evolve like $|0_L\rangle \rightarrow \cos\phi\,|0_L\rangle + \sin\phi\,|1_L\rangle$ and $|1_L\rangle \rightarrow -\sin\phi\,|0_L\rangle + \cos\phi\,|1_L\rangle$, which corresponds to the logical rotation $\hat{R}^y_L(2\phi) \equiv \exp(i\phi\hat{\sigma}^y_L)$, where $\hat{\sigma}^y_L$ is the usual Pauli operator in the logical basis. It suffices now to show how to implement a logical rotation around any other axis. It is straightforward to see that, when acting on $\mathbb{V}_{DFS}$, the following identity holds: $\hat{R}^z_L(\theta) \equiv c_s\hat{\sigma}^x_p.\hat{R}^x_s(-\theta).c_s\hat{\sigma}^x_p$, where $p$ and $s$ refer to the polarization and spatial mode qubits, respectively. For example, $c_s\hat{\sigma}^x_p$ is a controlled-not gate, where the polarization qubit is controlled by the spatial mode qubit. Finally, it is important to notice that, in contrast to $\hat{R}^y_L(2\phi)$, where the evolution takes place entirely inside $\mathbb{V}_{DFS}$, in the case of $\hat{R}^z_L(\theta)$ the evolution is not fault-tolerant, meaning that $\hat{R}^z_L(\theta)$ takes the protected states momentarily out of $\mathbb{V}_{DFS}$ and then brings them back. Nevertheless, this is of no consequence here, since $\hat{R}^z_L(\theta)$ is never applied during the transmission but at one of the user's laboratories, where the reference frame is perfectly defined.

*Quantum key distribution.* One immediate application of the ideas developed above is the implementation of single-photon quantum key distribution schemes which do not require initial alignment of the preparation and measurement systems. As an example, let us briefly outline the BB84 [17] protocol using these single–photon logical qubits. By choosing randomly between the angles $\phi_A = \{0, \pi/4\}$ and applying the rotation $\hat{R}^y_L(2\phi_A)$, Alice can send random bits in either the logical computational basis or the rotated logical basis $|\pm_L\rangle = (|0_L\rangle \pm |1_L\rangle)/\sqrt{2}$. Bob's random measurements in the computational or rotated logical bases, in turn, are carried out by simply performing the logical rotations $\phi_B = \{0, -\pi/4\}$ and subsequently detecting –unambigously and with perfect efficiency– in the computational logical basis $B_L$ with the single-photon Bell-state measurement (BSM) technique mentioned above.

*Generation of entangled logical states.* Using SPDC, it is possible to create two-photon states entangled in both polarization and transverse HG modes [18, 19]. Pumping a single type-I crystal with a Gaussian profile beam and post-selecting only the first-order modes, one can generate down-converted photons in the entangled state $(|Hh_1Hh_2\rangle + |Hv_1Hv_2\rangle)/\sqrt{2}$, where the subindices 1 and 2 refer to photons in different (longitudinal) momentum modes. Using controlled operations on the physical qubits, it is possible to transform this state to an entangled logical state. It is easy to show that applying the following sequence of gates $c_s\hat{\sigma}^x_p.\hat{h}_s.c_s\hat{\sigma}^x_p$ to the phys-

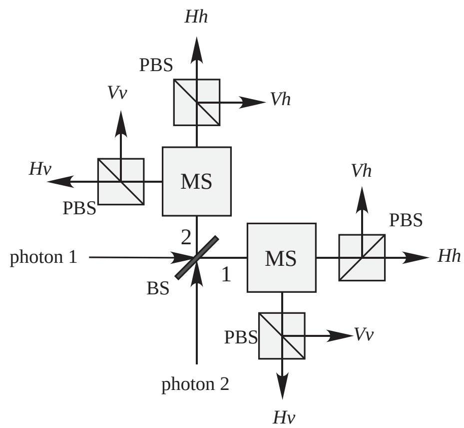


FIG. 2: Bell-state measurement device for logical qubits using a 50-50 beam splitter (BS). MS is a transverse mode sorter and PBS a polarizing beam splitter.

ical qubits of each photon transforms the SPDC output state to the two-photon Bell state composed of single-photon logical qubits: $\left|\Phi_L^+\right\rangle = (|0_{L_1}0_{L_2}\rangle + |1_{L_1}1_{L_2}\rangle)/\sqrt{2}$. Here $\hat{h}_s$ is a Hadamard gate on the spatial mode qubit. The other three logical Bell states, $\left|\Phi_L^-\right\rangle = (|0_{L_1}0_{L_2}\rangle - |1_{L_1}1_{L_2}\rangle)/\sqrt{2}$ and $\left|\Psi_L^\pm\right\rangle = (|0_{L_1}1_{L_2}\rangle \pm |1_{L_1}0_{L_2}\rangle)/\sqrt{2}$, can be immediately obtained from $\left|\Phi_L^+\right\rangle$ with the single logical qubit rotations described before. An alternative method to generate an entangled logical state employs the methods proposed in Ref. [19] using a second-order HG pump beam. We note that this method can also be used to create non-maximally entangled logical states.

*Tests of quantum nonlocality.* An important application of the entangled logical states just presented is the implemention of tests of Bell's theorem without the usual alignment of the analyzers, with only two photons. Furthermore, using non-maximally entangled logical states, one can implement alignment-free tests of Hardy's nonlocality without inequalities [20]. The importance of such tests has been pointed in [6], where a scheme using eight photons was proposed. Also, the ability to realize these tests allows for alignment-free implementations of entanglement-based quantum cryptography [21].

*Bell state measurement.* The main ingredient to quantum teleportation and dense coding is a BSM on two qubits. In previous experiments using qubits encoded in single DOF of photons, a partial BSM was performed using two-photon interference [22, 23]. Here we present a device which can be used to perform a partial BSM on the logical qubits presented here. FIG. 2 illustrates our analyzer. Photons are input on opposite sides of a 50-50 beam splitter (BS). It has been shown that, in addition to the $\pi$ phase shift present in the usual beam splitter transformations, the transverse spatial mode $|h\rangle$ acquires an additional $\pi$ phase due to reflection from the BS [13]. That is, the evolution operator of a $50-50$ BS is $\hat{B} \equiv e^{i\frac{\pi}{2}(\hat{a}_{Hv}\hat{b}^\dagger_{Hv}+\hat{a}^\dagger_{Hv}\hat{b}_{Hv})} \otimes e^{i\frac{\pi}{2}(\hat{a}_{Vv}\hat{b}^\dagger_{Vv}+\hat{a}^\dagger_{Vv}\hat{b}_{Vv})} \otimes e^{-i\frac{\pi}{2}(\hat{a}_{Hh}\hat{b}^\dagger_{Hh}+\hat{a}^\dagger_{Hh}\hat{b}_{Hh})} \otimes e^{-i\frac{\pi}{2}(\hat{a}_{Vh}\hat{b}^\dagger_{Vh}+\hat{a}^\dagger_{Vh}\hat{b}_{Vh})}$, where $\hat{a}^\dagger_{Xx}$ and $\hat{b}^\dagger_{Xx}$ are the creation operators of one photon with polarization $X$ ($=H$ or $V$) and HG mode $x$ ($=h$ or $v$), in momentum mode 1 and 2, respectively (notice the different signs in the exponents for the cases $Xh$ and $Xv$). Upon application of $\hat{B}$ our logical states transform as:

$$\begin{aligned}
\left|\Psi_L^-\right\rangle \to \frac{1}{4}[(&|Hv_1Hh_2\rangle - |Hh_1Hv_2\rangle - |Hv_1Vv_1\rangle \\
&- |Hv_2Vv_2\rangle - |Vh_1Hh_1\rangle - |Vh_2Hh_2\rangle - |Vh_1Vv_2\rangle \\
&+ |Vv_1Vh_2\rangle) - (|Hh_1Hv_2\rangle - |Hv_1Hh_2\rangle \\
&+ |Hh_1Vh_1\rangle + |Hh_2Vh_2\rangle + |Vv_1Hv_1\rangle \\
&+ |Vv_2Hv_2\rangle - |Vv_1Vh_2\rangle + |Vh_1Vv_2\rangle)] \,, \quad (1)
\end{aligned}$$

$$\begin{aligned}
\left|\Psi_L^+\right\rangle \to \frac{1}{4}[(&|Hv_1Hh_1\rangle - |Hh_2Hv_2\rangle + |Hv_1Vv_2\rangle \\
&+ |Vv_1Hv_2\rangle - |Vh_1Hh_2\rangle - |Hh_1Vh_2\rangle + |Vh_1Vv_1\rangle \\
&- |Vh_2Vv_2\rangle) + (|Hh_1Hv_1\rangle - |Hh_2Hv_2\rangle \\
&- |Hh_1Vh_2\rangle - |Vh_1Hh_2\rangle + |Vv_1Hv_2\rangle \\
&+ |Hv_1Vv_2\rangle - |Vv_2Vh_2\rangle + |Vv_1Vh_1\rangle)] \,, \quad (2)
\end{aligned}$$

$$\begin{aligned}
\left|\Phi_L^\pm\right\rangle \to \frac{1}{4}[(&|2Hv_1\rangle - |2Hv_2\rangle - \sqrt{2}\,|Vh_1Hv_2\rangle \\
&- \sqrt{2}\,|Hv_1Vh_2\rangle - |2Vh_1\rangle + |2Vh_2\rangle) \\
&\pm (|2Hh_2\rangle - |2Hh_1\rangle + \sqrt{2}\,|Hh_1Vv_2\rangle \\
&+ \sqrt{2}\,|Vv_1Hh_2\rangle + |2Vv_1\rangle - |2Vv_2\rangle)] \,. \quad (3)
\end{aligned}$$

Using additional linear optics devices to separate $H$ from $V$ and $h$ from $v$, it is possible to separate photons in different states. For example, events like $|Vh_1Hh_1\rangle$, corresponding to two photons in the same transverse mode and same output port of the BS, can still be separated by polarization, and registered through two-photon coincidence detections. The states $\left|\Psi_L^-\right\rangle$ and $\left|\Psi_L^+\right\rangle$ always give coincidences in different modes, so that they can be detected and discriminated with perfect efficiency. On the other hand, $\left|\Phi_L^-\right\rangle$ and $\left|\Phi_L^+\right\rangle$ give coincidence events 50 % of the time [24]. These events are the same for both states, so they still cannot be discriminated from one another. Still, this BSM of logical qubits can be used for the implementation of quantum dense coding, allowing for the transmission of $\log_2 3$ bits of information in a single logical qubit, with an overall efficiency of $1-\frac{1/3}{2}\approx 0.83$ with coincidence detections.

*Quantum teleportation.* Quantum teleportation [25] is perhaps the most important application of a BSM. For example, the error probability in the transmission of a qubit scales exponentially with the length of the channel, seriously limiting quantum communications. One way to circumvent this is using a quantum repeater [26], in which the channel between $A$ and $B$ is divided into $N$ segments using $N$ entangled pairs. Since the procedure requires $N-1$ teleportation protocols, $N$ SRF's are necessary. Therefore it is apparent that a SRF-free quantum teleportation scheme is of considerable importance, since

it would greatly reduce the overhead of the repeater.

Suppose that $A$ and $B$ share the entangled logical state $\left|\Phi_L^+\right\rangle_{12}$ between logical qubits 1 and 2, but do not a share common reference frame; and $A$ would like to teleport a third logical qubit $|\psi_L\rangle_3 = \alpha\,|0_L\rangle_3 + \beta\,|1_L\rangle_3$ to $B$. Using the BSM presented above, $A$ can project logical qubits 1 and 3 onto the logical Bell basis, and can identify $\left|\Psi_L^\pm\right\rangle$ unambiguously with 100% efficiency. She then communicates her measurement result to $B$, who applies the logical operations $\hat{\sigma}_L^x$ or $\hat{\sigma}_L^z\hat{\sigma}_L^x$ to his logical qubit when the measurement result is $\left|\Psi_L^+\right\rangle$ or $\left|\Psi_L^-\right\rangle$, respectively. The overall teleportation efficiency is 50%, and the teleportation fidelity is 1. Nevertheless, $A$ and $B$ can increase the efficiency of the protocol, while still working in the coincidence basis, at the cost of a slight decrease in fidelity. Half of the time, $A$'s BSM corresponds to one of the $\left|\Phi_L^\pm\right\rangle$ states, which, in turn, give coincidence detections 50% of the time. In these cases, $A$ can inform $B$ that the measurement result was $\left|\Phi_L^\pm\right\rangle$, and then $B$ knows that his logical qubit is either in state $\alpha\,|0_L\rangle + \beta\,|1_L\rangle$ (with probability 1/2, corresponding to a teleportation fidelity of 1) or in $\alpha\,|0_L\rangle - \beta\,|1_L\rangle$ (probability 1/2, corresponding to an average teleportation fidelity of 2/3). Thus, if they perform the teleportation protocol only when $A$ detects a coincidence event, the efficiency is improved to 75% and the overall fidelity of the teleportation procedure is $2/3\times1+1/3\times1/2\times1+1/3\times1/2\times2/3 = 17/18 \approx 94.4\%$.

*Discussion.* In addition to rotations due to user misalignment, there is also the problem of decoherence of the physical qubits. The atmosphere is not birefringent, so random polarization rotations are not an issue in free space propagation of photons. However, fluctuations of the refractive index of the atmosphere can deform the transverse modes. Nonetheless, these effects could be monitored using an intense reference beam, and then corrected. Optical fibers preserve spatial mode but are birefringent, which severely limits long-distance quantum communication with polarization qubits. Depending on the communication protocol, these polarization rotations can be overcome using a "plug and play" setup [27].

We thank L. Davidovich for reading the manuscript and acknowledge financial support from the CNPq, CAPES, FAPERJ, and the Brazilian Millennium Institute for Quantum Information.

[1] A. Peres, P. F. Scudo, Phys. Rev. Lett. **86**, 4160 (2001); G. Chiribella *et al.*, Phys. Rev. Lett. **93**, 180503 (2004).
[2] Z. D. Wallton *et al.*, Phys. Rev. Lett. **91**, 087901 (2003).
[3] J.-C. Boileau *et al.*, Phys. Rev. Lett. **93**, 220501 (2004); Q. Zhang *et al.*, Phys. Rev. A. **73**, 020301(R) (2006).
[4] T.-Y. Chen *et al.*, Phys. Rev. Lett. **96**, 150504 (2006).
[5] J.-C. Boileau *et al.*, Phys. Rev. Lett. **92**, 017901 (2004).
[6] A. Cabello, Phys. Rev. Lett. **91**, 230403 (2003).
[7] S. D. Bartlett, T. Rudolph, R. W. Spekkens, Phys. Rev. Lett.**91**, 027901 (2003).
[8] M. Fiorentino, F. N. C. Wong, Phys. Rev. Lett. **93**, 070502 (2004).
[9] G. M. Palma, K. A. Suominen, A. K. Ekert, Proc. R. Soc. London, Ser. A **452**, 567 (1996); A. Barenco *et al.*, **SIAM J.** Comp. **26**, 1541 (1997); P. Zanardi, M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
[10] D. Kielpinski *et al.*, Science **291**, 1013 (2001).
[11] P. G. Kwiat, J. Mod. Optics **44**, 2173 (1997).
[12] J. T. Barreiro *et al.*, Phys. Rev. Lett. **95**, 260501 (2005).
[13] A. N. de Oliveira, S. P. Walborn, C. H. Monken, J. Optics B: Quantum and Semiclassical Optics **7**, 288 (2005).
[14] A. T. O'Neil, J. Courtial, Opt. Comm. **181**, 35 (2000).
[15] H. Sasada, M. Okamoto, Phys. Rev. A. **68**, 012323 (2003).
[16] M. W. Beijersbergen *et al.*, Optics Comm. **96**, 123 (1993).
[17] C. H. Bennett, G. Brassard, Proc. IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 175 (1984).
[18] N. K. Langford *et al.*, Phys. Rev. Lett. **93**, 053601 (2004).
[19] S. P. Walborn, S. Pádua, C. H. Monken, Phys. Rev. A **71**, 053812 (2005).
[20] L. Hardy, Phys. Rev. Lett. **71**, 1665 (1993).
[21] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); C.H. Bennett, G. Brassard, N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[22] K. Mattle *et al.*, Phys. Rev. Lett. **76**, 4656 (1996).
[23] D. Bouwmeester *et al.*, Nature **390**, 575 (1997).
[24] In [22], 50%-efficiency coincidence detection of the states $\left|\Phi^\pm\right\rangle$ was achieved putting an additional BS and detector in every spatial output, which doubles the number of BSs and detectors. Using the same number of detectors, our analyzer allows us to measure in the logical Bell basis with the same detection efficiency for $\left|\Phi_L^\pm\right\rangle$ as in [22].
[25] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
[26] H. J. Briegel *et al.*, Phys. Rev. Lett. **81**, 5932 (1998).
[27] H. Zbinden *et al.*, Electron. Lett. **33**, 586-588 (1997).